NC DIT
NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

2019 Cyber Awareness Symposium

CYBER EXPOSURE:
Relating Critical Functions, Threats, Assets, & Vulnerabilities

Robert Huber
CHIEF SECURITY OFFICER

TYPICAL DAY

ALARM GOES OFF
Grab phone

SLACK
Check Slack for incidents

EMAIL
Check email for tickets/incidents

NEWS
Quick scan of the news

CYBER NEWS
Quick scan of cyber security specific news/alerts (combatting WSJ effect)

certnz

threatpost

Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

BLOG

AusCERT

tenable

Incident

POTENTIAL COMPROMISE

Employee downloaded a malicious file from their personal email account.

When I review the incident the questions I ask the team are as follows…

1 Does the employee have administrative access?

2 Do they have access to critical or sensitive data?

3 Did you review other activity associated with the account?

4 Did the malware exploit a vulnerability?

How many other assets have the same vulnerability?
Check Tenable.io/Tenable.SC

What other vulnerabilities does this asset have? ***Check Tenable.io/Tenable.SC***

Is a patch available for the vulnerability?
Check Tenable.io/Tenable.SC

Do we have any threat intel indicating prevalence or targeting for this malware or vulnerability? ***Predictive Prioritization***

Do any of our other detection/protection mechanisms mitigate the vulnerability?

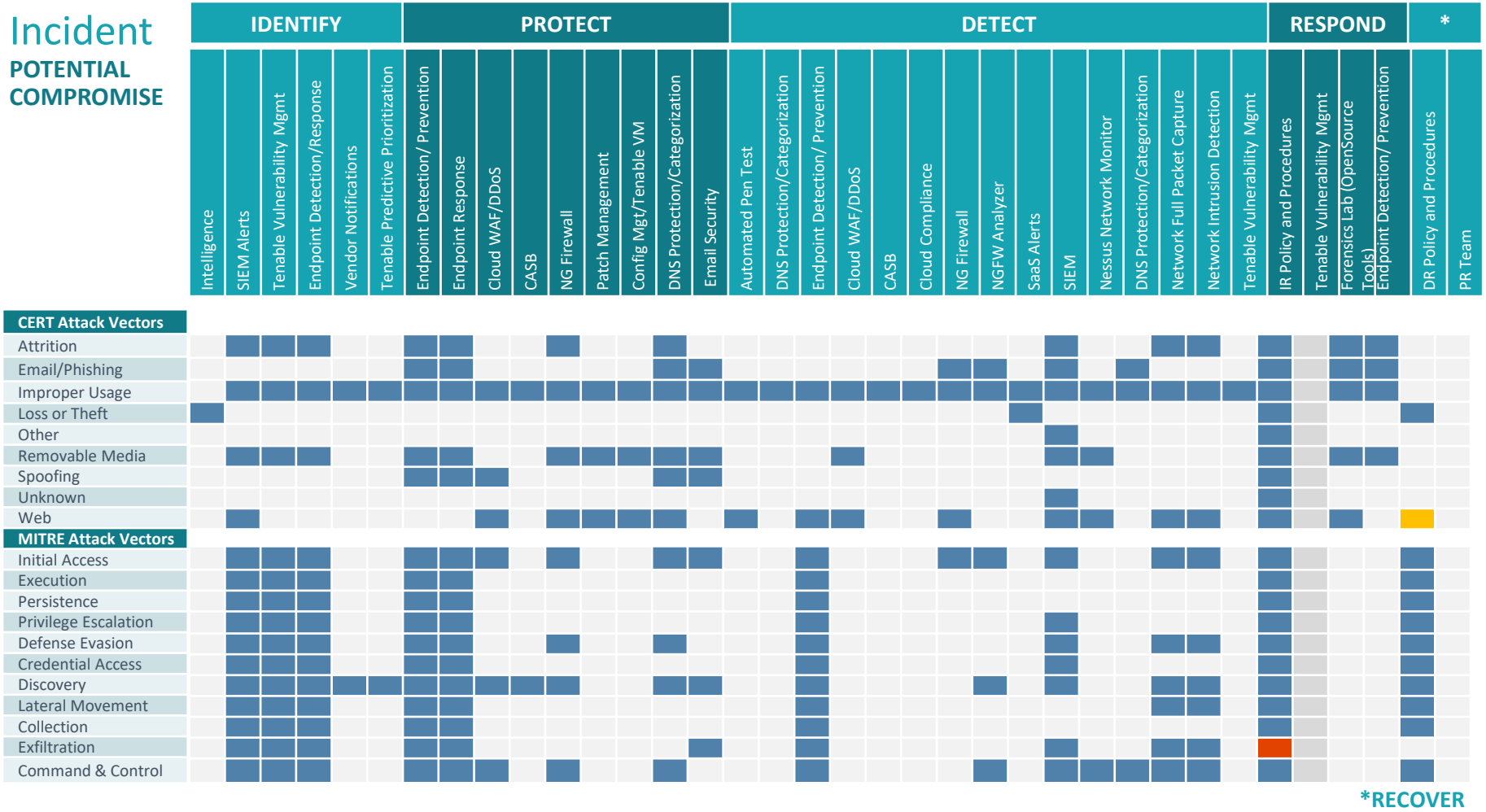
Do we need to send out a corporate communication?

Do we need to inform employees, vendors, partners, etc.?

tenable

Incident

POTENTIAL COMPROMISE



*RECOVER

Incident

CRITICAL VULNERABILITY

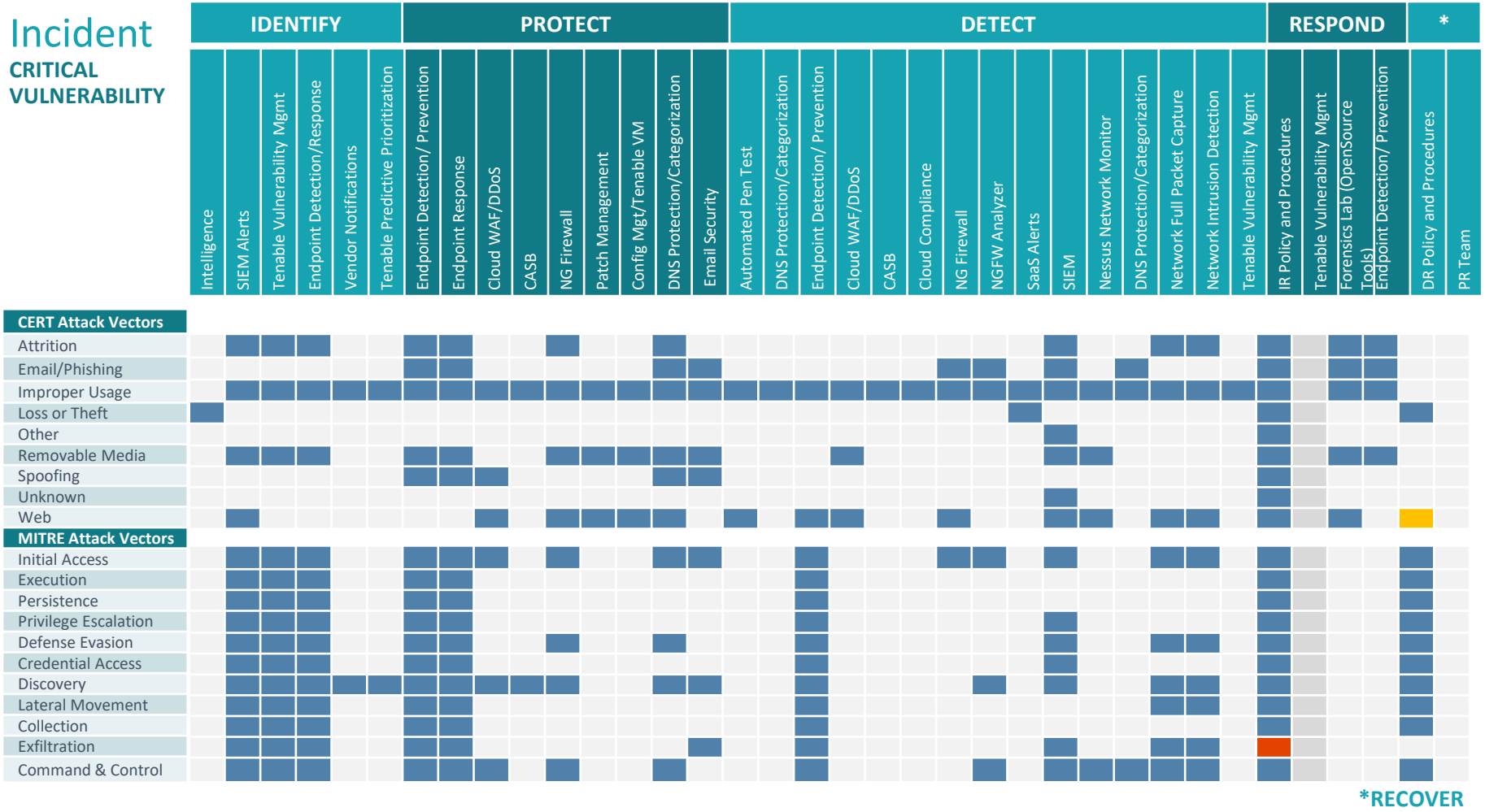
Critical vulnerability is announced for Linux systems

When I review the vulnerability the questions I ask the team are as follows …

1. How many other assets have the same vulnerability?
   Check Tenable.io/Tenable.SC
2. How many of our those assets are considered critical?
   Check Tenable.io/Tenable.SC (asset tagging/grouping – now our source of truth)
3. How many are of those assets are externally facing?
   Check Tenable.io/Tenable.SC (asset tagging/grouping)
4. Is an exploit available or what is the likelihood of an exploit?
   Threat intelligence/Tenable Vulnerability Priority Rating (VPR)
5. What is the ease of exploitation?
   Predictive Prioritization
6. Is a patch available for the vulnerability?
   Check Tenable.io/Tenable.SC
7. Do we have any threat intel indicating prevalence or targeting for this malware or vulnerability? ***Tenable VPR***
8. Do any of our other detection/protection mechanisms mitigate the vulnerability?
9. Do we need to send out a corporate communication?

Incident

CRITICAL VULNERABILITY



*RECOVER

AUDITS

EVIDENCE REQUESTS

FINDINGS TO ADDRESS:

- BYOD Policies
- Security Strategy/Management
- Physical Security – staff passes

tenable

SECURITY ASSESSMENT QUESTIONNAIRES (SAQs)

Ref	Question	Please provide as full a response as you can which supports how you meet this requirement
IS13.3	Please describe the process you follow for the validation and remediation of any findings identified as part of the penetration test	Remediation is tracked via a ticket which is created for each vulnerability/weakness discovered during the Pen Test. Progress is tracked to completion and subsequently the ticket(s) will be closed.
IS14	Please describe the process and output of all network vulnerability scans performed.	Vulnerability scans follow the Vulnerability Management Policy. See Policy for additional details.
IS14.1	Please confirm if your vulnerability scans cover:- - all internal & external network ranges on a monthly basis - cover all network components eg. switches, routers etc - be approved by an Approved Scanning Vendor where appropriate - devices not scanned are raised as issues	Sources of vulnerability findings are derived from both SecurityCenter and Tenable.io products to ensure complete coverage, including: 1. Nessus vulnerability scans 2. Nessus Network Monitor (NNM) continuuous monitoring 3. Results of internal or third party penetration testing 4. Log Correlation Engine (LCE) events 5. Web applications scans 6. Vulnerabilities reported by the United States Computer Emergency Readiness Team (USCERT)
IS14.2	Please describe the controls operated regarding the remediation of any vulnerability scan findings	Discovered vulnerabilities are remediated based on vulnerability management policy. High and Critical vulnerabilities are given priority. These findings are considered proprietary and we are unable to distribute to customers.

SCREENSHOT

THIS IS A SLICE FROM

1 SAQ

7 TABS | **130+ QUESTIONS**

WE RECEIVED

48 SAQs

IN **Q4 2018 ALONE!**

tenable

Customer Contracts

Typical Contract Language

d) Remove from service and the network any workstation, file, disk or other resource on which a virus, threat or security vulnerability is detected until the issue is resolved.

e) **Maintain a periodic vulnerability testing of Supplier's network, infrastructure and applications, regardless of dedicated or non-dedicated networks, and vulnerabilities are to be remediated in accordance with the following timetable:**

- Critical Vulnerabilities within 72 hours of identification.
- High Vulnerabilities within 30 days of identification (CVSS of 7.0-10.0)
- Medium Vulnerabilities within 60 days of identification (CVSS of 4.0-6.9)
- Low Vulnerabilities within 90 days of identification (CVSS of 0.0-3.9.0)

SUPPLY CHAIN RISK MANAGEMENT

	IT Risk & Security Assessment Questionnaire (SAQ)
	Tenable Network Security, Inc. ("Tenable") has a responsibility to ensure all information associated with the company and our customers is appropriately protected during the handling, transmission, storage or processing by a third party organizaiton.
	This questionnaire is part of the Tenable risk review process for third parties, intended to identify and understand the control environment in place for managing the protection of information in external custody.
	SAQ (this worksheet): Please answer all questions and provide relevant explanation or detail in the 'Further Information' column. Where necessary, please provide copies of, or extracts from, supporting policy or procedure documents.
	Scope: This form is only required for companies that are not ISO or SOC 2 Type II compliant. For companies that are ISO or SOC 2 Type II compliant, please provide an attestation of your compliance along with a security whitepaper.
1	Contact Information
1.1	Company's full legal name
1.1	Date of completion
1.11	Briefly outline the service that your company does (or will) provide to Tenable.
1.12	Briefly describe relevant systems/applications (in terms of the platforms, technologies, architecture).
1.13	List the physical locations where Tenable information will be stored.
1.2	Your name
1.3	Job title
1.4	E-mail address
1.5	Telephone number
2	Basic Requirements
2.1	Is your company certified to information security or auditing standards, such as ISO27001 or SSAE16
2.1	Does your company have a documented process for responding to security incidents?
2.11	Does this process ensure that security incidents are reported through to the appropriate channels to Tenable?
2.2	Have you been independently audited in any other way?

SCREENSHOT

Requests from employees for new software/ SaaS/contractor

2.1 Do they have a SOC 2 Type 2 report, recent ISO 27001 audit?

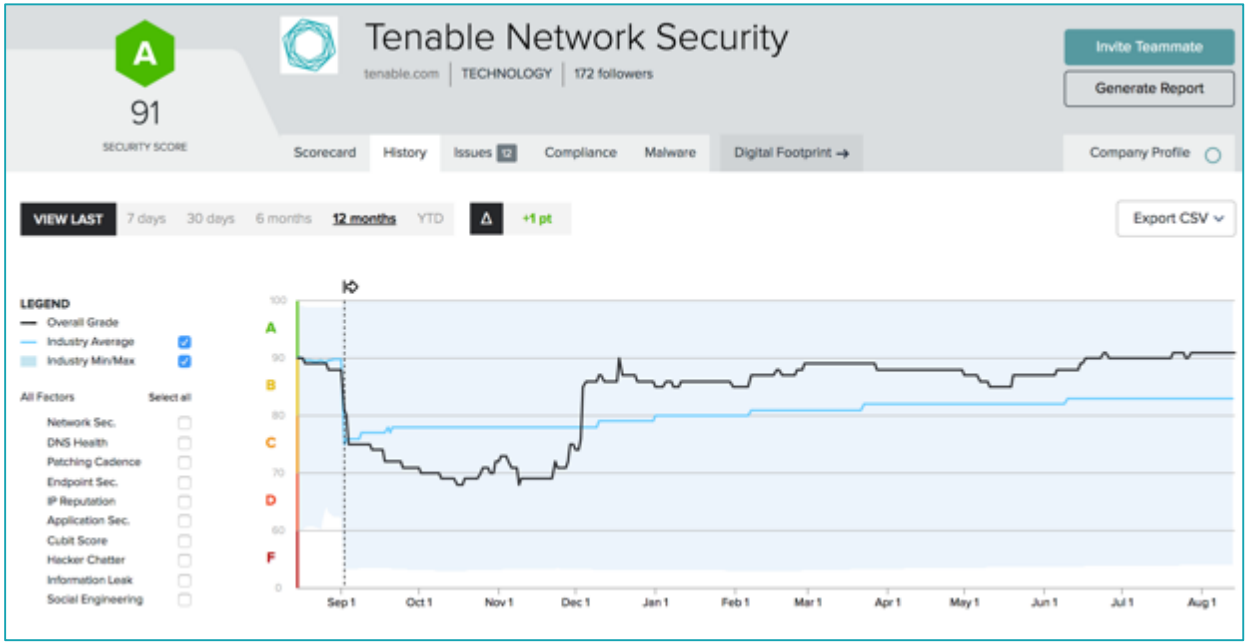
IF NOT, COMPLETE OUR SAQ

ANSWER 90+ QUESTIONS

tenable

3rd Party Scorecards

Customer and Partner 3rd party vendor procurement and security assessment teams monitor our scores - so we must.



SCREENSHOTS

tenable

PRODUCT SECURITY

From the field:

Customer is looking for verification of proper security testing for vulns, exploits, etc. in our product. They don't need specific findings but an executive summary of how we test the security of our products.

SECURE SDLC PROCESS

Proactive identification of security issues in our products, can you triage, assess and report mitigations and/or plans to address?

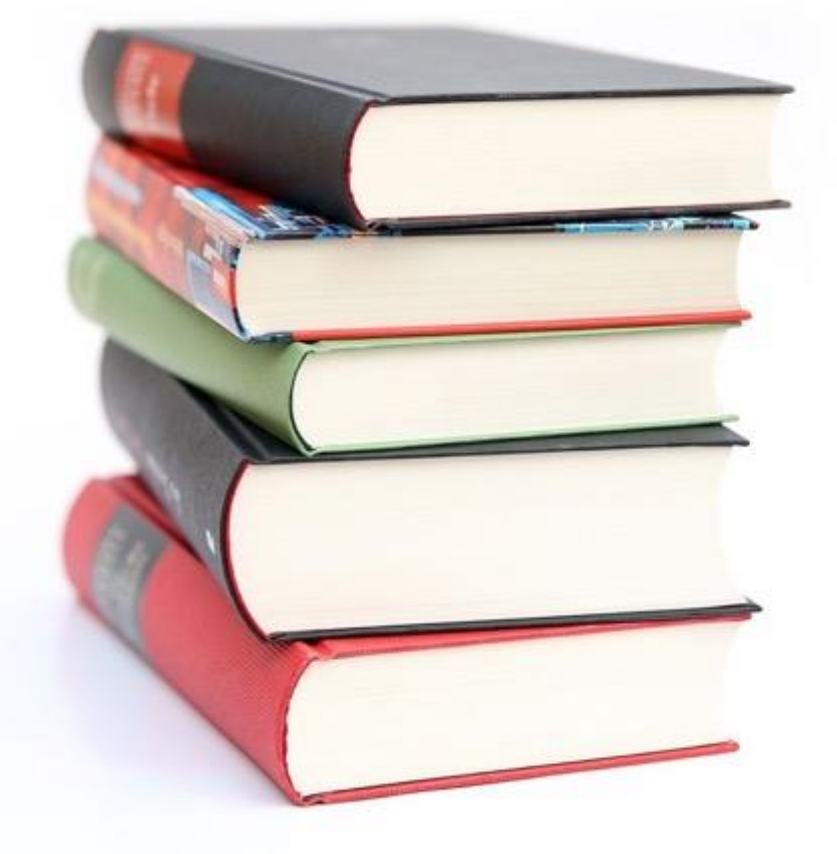
Cyber Exposure

WHAT DO I NEED TO IDENTIFY CYBER EXPOSURE?

To combine all these things….

tenable


FOCUS ON WHAT MATTERS FIRST



risk *noun*

\ˈrisk \

1. : possibility of loss or injury : PERIL
2. : function of :
   : ASSETS
   : THREATS
   : VULNERABILITIES

tenable

static *adjective*

\stat-ik \

1. : pertaining to or characterized by a fixed or stationary condition
2. : showing little or no change

tenable

CYBER EXPOSURE

"Cyber Exposure is an emerging discipline for managing and measuring cybersecurity risk in the digital era.

Cyber Exposure transforms security from static and siloed visibility into cyber risk to dynamic and holistic visibility across the modern attack surface."

Asset Prioritization

IN THE PRIVATE SECTOR

BUSINESS IMPACT ANALYSIS

Identify at a high level impact to key locations, personnel or systems given a disruption, considering the following:

FINANCIAL IMPACTS

OPERATIONAL IMPACTS

MANAGEMENT TOLERANCES

RESOURCE DEPENDENCIES

tenable

BIA: Critical Functions, Assets, Services

BUSINESS CONTEXT

- Client data and services
- External websites
- CRM
- Productivity suite
- Code repositories
- Key personnel & facilities

Key Risk Indicators (KRIs)

EXAMPLES WITH KPIs

Tenable.io customer vulnerability data disclosure

VISIBILITY, VULNERABILITIES AND MISCONFIGURATIONS IN T.IO INFRASTRUCTURE

Loss of intellectual property (code repos)

ACCESS CONTROLS, CRITICAL EVENTS IDENTIFIED AND MONITORED

Strategic information leak (G Suite)

VISIBILITY, CRITICAL EVENTS IDENTIFIED AND MONITORED, ACCESS CONTROLS

Damage to brand or reputation (external websites)

PENETRATION TESTS, WAS, VM, AMBIONICS

Sales information leakage (Salesforce)

VISIBILITY, CRITICAL EVENTS IDENTIFIED AND MONITORED, ACCESS CONTROL

tenable

Asset Prioritization

IN THE PUBLIC SECTOR

National Risk Management Framework

IDENTIFY

ANALYZE

PRIORITIZE

MANAGE

- **3,300** electricity utilities in the U.S.
- **32 EMCs in NC, 76 municipally owned**
- **~70%** of customers get their electricity from IOUs

- **16,000** publicly owned wastewater treatment plants in operation across the country
- **87%** of US are served by publicly owned water/waste
- **NC regulates 90+ Water/Sewer entities**

- **7,700** organizations provide public transportation in the U.S.

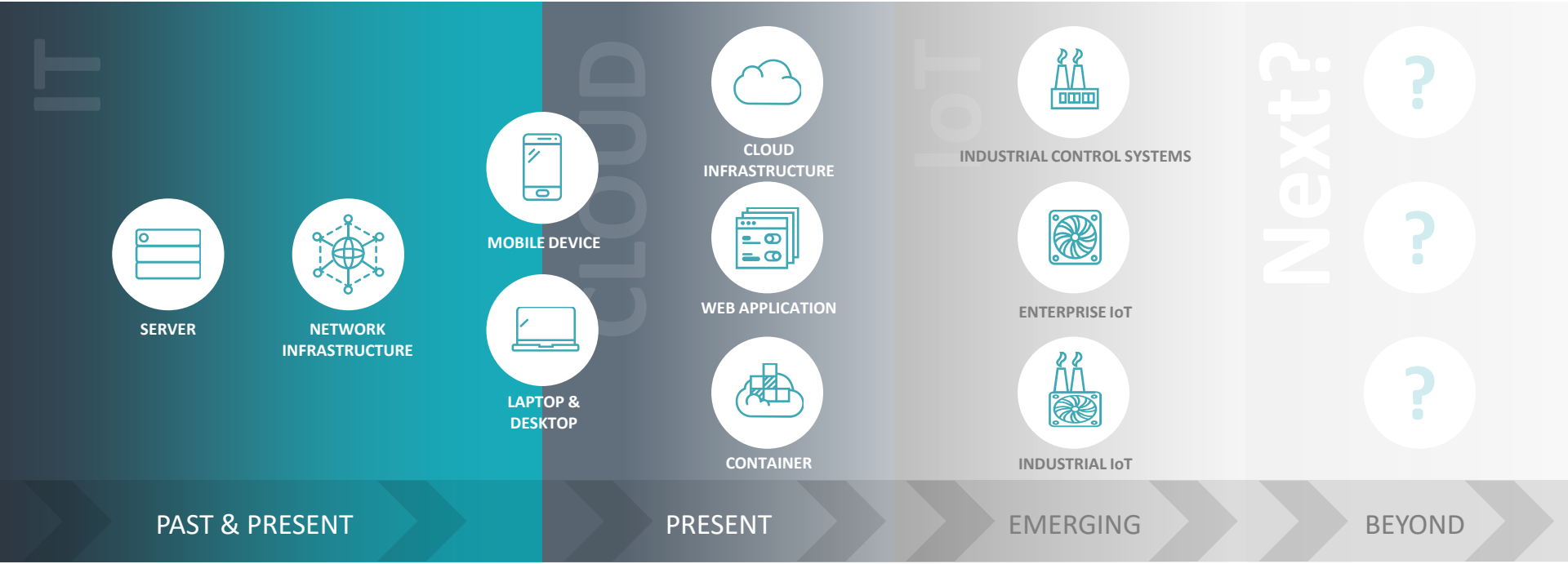
- There are **1,830,672** miles of oil and gas pipelines across the U.S.
- **8 municipal gas systems in NC**

- Cross sector dependencies

tenable

ASSETS

Digital transformation has made asset and vulnerability identification **DIFFICULT**



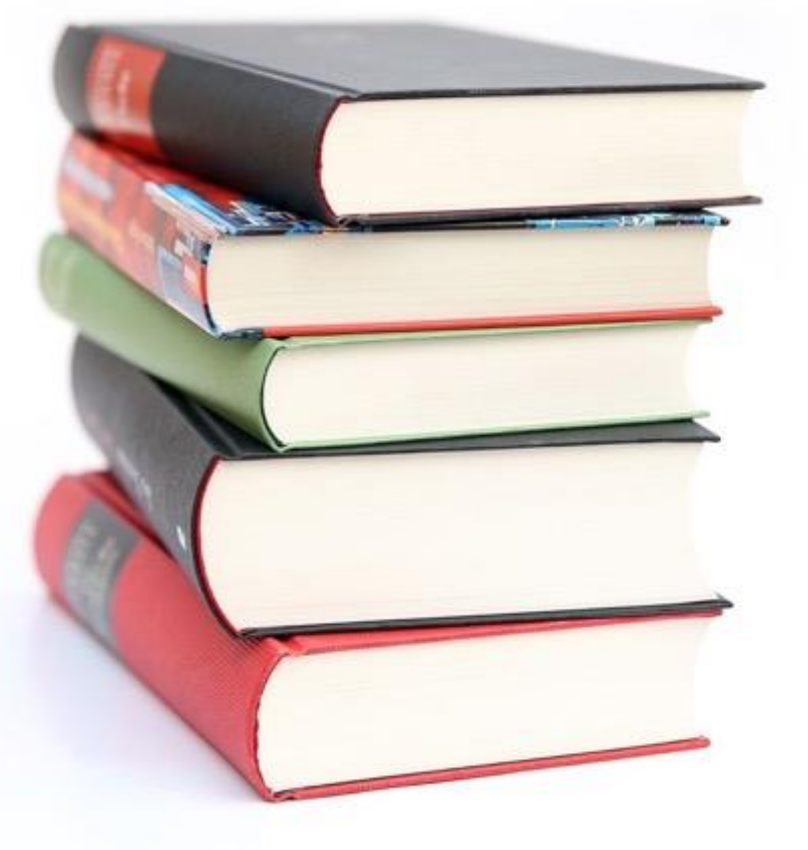
tenable

Threat Prioritization

Data science can measure elements that impact threat intent, capability, and opportunity:

- Threat recency
- Threat intensity
- Exploits available
- Previous attacks/TTPs
- Complexity
- Darkweb, forums, blogs, code repos

tenable



risk *noun*

\ˈrisk \

1. : possibility of loss or injury : PERIL
2. : function of :
   : ASSETS
   : **THREATS**
   : VULNERABILITIES

tenable

16,500

VULNERABILITIES DISCLOSED IN 2018

7%

of vulnerabilities had an exploit available

63%

of vulnerabilities discovered in environments are CVSS 7+

12%

of vulnerabilities disclosed in 2017 were CVSS 9+

Vulnerability Intelligence Report Tenable Research

If Everything Is Important — NOTHING IS

59%

High or **Critical**

Vulnerability Intelligence Report Tenable Research

tenable

VPR

VULNERABILITY PRIORITY RATING

Leverages supervised machine learning algorithms to calculate the priority of a vulnerability based on the real threat posed.

Key Drivers include

Threat Recency

Threat Intensity

Exploitability

Vulnerability Age

Threat Sources

Cyber Exposure

WHAT DO I NEED TO IDENTIFY CYBER EXPOSURE?

To combine all these things….

tenable


FOCUS ON WHAT MATTERS FIRST

Prioritize based on importance of asset AND risks posed by vulnerabilities on the asset

VPR + **ACR**

VULNERABILITY PRIORITY RATING

ASSET CRITICALITY RATING

Leverage machine learning and threat intelligence to prioritize vulnerabilities based on real world risk

Prioritize assets based on indicators of business value and criticality

Focus First On What Matters Most

Remediation Guidance

Recommended Workflows

Drill down into specific vulnerabilities and assets for business and technical context to enable more effective remediation.


Business Context


Technical Context

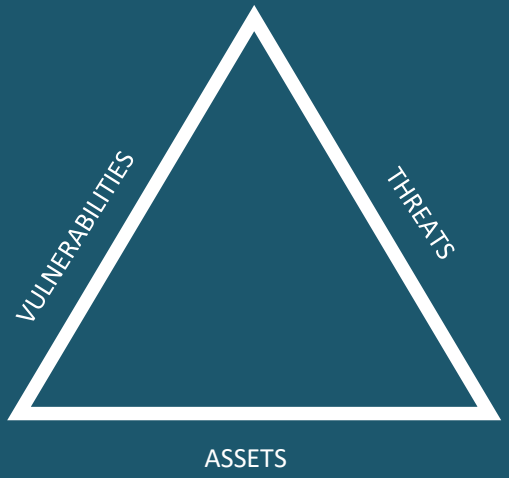

Specific Assets

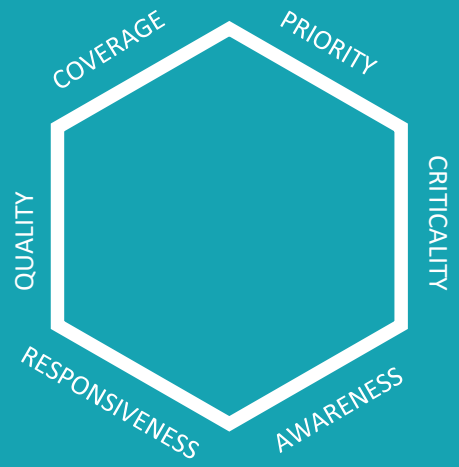

Workflow Guidance

cyber risk *noun*

\cy•ber'risk \

1. : risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems
2. : function of :





cyber exposure *noun*

\cy•ber'ex·po·sure\

1. : an emerging discipline for managing and measuring cybersecurity risk
2. : function of :